1 AUSA for second AUSA

AO106 (Rev. 12/03) Affidavit for Search Warrant

UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF CALIFORNIA

In the Matter of the Search of
(Name, address or brief description of person, property or premises to be searched)

ONE (1) LAPTOP COMPUTER
GREY OR BLACK IN COLOR

ONE (1) DIGITAL CAMERA

APPLICATION AND AFFIDAVIT FOR SEARCH WARRANT

Case Number: '07 MJ 8968

I, Timothy Ballard being duly sworn depose and say:

I am a(n) Special Agent with U. S. Immigration & Customs Enforcement and have reason to believe
Official Title

that ☐ on the person of or ☑ on the property or premises known as (name, description and/or location)

REFER TO ATTACHMENT A

in the SOUTHERN District of CALIFORNIA

there is now concealed a certain person or property, namely (describe the person or property to be seized)

REFER TO ATTACHMENT B

which is (state one or more bases for search and seizure set forth under Rule 41(c) of the Federal Rules of Criminal Procedure)

evidence of a criminal offense which has been used as the means for committing a criminal offense.

concerning a violation of Title 18 United States code, Section(s) 2252

The facts to support a finding of probable cause are as follows:

REFER TO ATTACHED AFFIDAVIT OF ICE SPECIAL AGENT TIMOTHY BALLARD

FILED
DEC 06 2007
CLERK, U.S. DISTRICT COURT
SOUTHERN DISTRICT OF CALIFORNIA
BY EF DEPUTY

Continued on the attached sheet and made a part hereof: ☑ Yes ☐ No

[signature]
Signature of Affiant

Sworn to before me and subscribed in my presence,

DECEMBER 6, 2007	at	EL CENTRO	CALIFORNIA
Date		City	State

Peter C. Lewis	U.S.Magistrate Judge	[signature]
Name of Judge	Title of Judge	Signature of Judge

ATTACHMENT A

DESCRIPTION OF PROPERTY TO BE SEARCHED

A laptop computer, grey or blackish in color, and a digital camera belonging to Neil MORGAN, which are located in Neil MORGAN's bedroom. The house is located at1601 Drew Road, El Centro, CA, 92243 and is more particularly described as a one story, doublewide mobile home, with blue, wood siding and white trim. The house has a carport attached to the left side of the house. Between the carport and the residence is a set of a few stairs leading to a door that accesses the left side of the residence. The house also contains a large porch at the center and right side of the home with a second door from the porch into the right side of the house. There is also a set of few stairs leading from the ground level of the right side of the house onto the porch, directly in front of the residence porch door on the right side. The number 39 is printed on a white placard and hangs on the front wall of the house. There is also a line of small bushes/trees with white flowers that sit directly in front of the residence.

Neil MORGAN's bedroom is located at the back of the house on the left or northern side of the house.

The subject premises is part of a larger mobile home community at 1601 Drew Road, which community is called Storm's Crossings. Though the mailing address for the subject premises is 1601 Drew Road, Lot 39, the community name for the small lane, which Space 39 is located on, is called Willow Lane.

ATTACHMENT B
ITEMS TO BE SEARCHED FOR AND SEIZED

A laptop computer, grey or black in color, and a digital camera that are located within the bedroom of Neil MORGAN, which bedroom is located within the premises detailed in Attachment A.

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

I, Senior Special Agent Timothy Ballard (hereinafter your "Affiant"), upon being duly sworn do hereby state that the following is true to my knowledge and belief:

1. I am a Special Agent with the U.S. Immigration and Customs Enforcement (ICE) having been so employed for approximately four years. I am currently assigned to the Cyber-crimes group within the ICE Office of Investigations, Office of the Assistant Special Agent in Charge, El Centro, California (ASAC/CA). I have assisted, or been the affiant, in the service of over twelve search warrants involving computer/cyber crimes. I received basic training from ICE regarding cyber-crime investigations. I have also completed the Internet Crimes Against Children Investigative Techniques training course, the ICE Cyber Crimes Center Child Exploitation Undercover Investigations training course, and additional child exploitation and computer investigative courses sponsored by the State of California's Office of Child Abuse Prevention and the Computer and Technology Crime High Response Team (CATCH). I am currently assigned to the Internet Crimes Against Children (ICAC) task force in San Diego, CA. This task force includes members of the San Diego Police Department, San Diego Sheriff's Department, U.S. Postal Inspection Service, Federal Bureau of Investigation, Naval Criminal Investigative Service, U.S. Attorney's Office and the San Diego District Attorney's Office.

2. This affidavit is offered in support of a search warrant application to search for a laptop computer and a digital camera belonging to Neil MORGAN within Neil MORGAN's bedroom at the MORGAN residence located at 1601 Drew Rd. Space 39, El Centro, CA, as more particularly described in Attachment "A" and to seize that laptop computer so as to subsequently search and analyze it for child pornography and other sexually explicit content related to child sex abuse and exploitation, as more particularly described in Attachment "B". The residence, 1601 Drew Rd, Space 39, El Centro, CA, is a doublewide mobile home, with blue siding and white trim. There is a carport attached to the left side of the house with a door from the carport into the home. There is a large porch at the center and left side of the home with a second door from the porch into the left side of the house. The number 39 is

printed on a white placard and hangs on the front wall of the house. Neil MORGAN's bedroom is located at the rear of the home and is the bedrrom located on the left, or the bedroom on the nortern-most side of the residence. The laptop computer is a dark/grey laptop last seen on the bed in Neil MORGAN's bedroom.

3. This affidavit is based upon information your Affiant has gained through training and experience, as well as upon information related to your Affiant by other individuals, including law enforcement officers. Since this affidavit is being submitted for the limited purpose of securing a search warrant, your Affiant has not included each and every fact known concerning this investigation but has set forth only the facts that your Affiant believes are necessary to establish probable cause to believe that evidence relating to violations of Title 18, United States Code §2252 et seq, are located on the laptop at the residence described above.

4. Based upon the following information, there is probable cause to believe that currently located within the above-described location, See Attachment "A", there is a laptop computer that contains evidence, fruits and instrumentalities of trafficking, receipt, distribution, manufacture and/or possession of visual depictions, and other related materials, involving minors engaging in sexually explicit conduct (child pornography), in violation of Title 18, United Stated Code §2252 et seq., said property more particularly described in Attachment "B."

5. As set forth above, Your Affiant has had both training and experience in the investigation of computer-related crimes. Based on that training, experience and knowledge, your Affiant knows the following:

A. The Internet is a worldwide network of computer systems operated by governmental entities, corporations, and universities. In order to access the Internet, an individual computer user must subscribe to an access provider, which operates a host computer system with direct access to the Internet. The World Wide Web (www) is a functionality of the Internet, which allows users of the Internet to share information;

B. With a computer connected to the Internet, an individual computer user can make electronic contact with millions of computers around the world. This connection can be made by any number of means, including modem, local area network, wireless and numerous other methods; and

C. The Gnutella network is used by persons who access the Internet to share files amongst each other. These types of networks are commonly referred to as peer-to-peer networks. Your Affiant knows through training and experience that peer-to-peer networks are frequently used to distribute child pornography.

D. And, in addition to Internet downloads of child pornography, a computer can be utilized to upload images of child pornography from CD's or other forms of digital media.

STATUTORY BACKGROUND

6. Title 18, United States Code, §2252 et seq., makes it a federal criminal offense to knowingly distribute, receive and/or possess any child pornography that has been mailed, shipped or transported in interstate or foreign commerce

SUMMARY OF INVESTIGATION

7. Your Affiant knows from training and experience that computers are a principle means of storing child pornography. These child pornography images may be downloaded to a computer via the Internet. Many times these images and video are downloaded via the Internet through file share programs, such as those that fall under open source, peer-to-peer networks or networks that are collectively known as the Gnutella network. Such Internet networks are frequently used in the trading of child pornography.

8. Through training and experience, your Affiant has learned that individuals who collect child pornography tend to be sexually attracted to children, their sexual arousal patterns and erotic

imagery focus, in part or in whole, on children. The collection may be exclusively dedicated to children of a particular age, gender, or other set of characteristics, or it may be more diverse, representing a variety of sexual preferences, including children. Child pornography collectors express their attraction to children through the collection of sexually explicit materials involving children as well as other seemingly innocuous material related to children. These individuals may derive sexual gratification from actual physical contact with children as well as from fantasies involving the use of pictures or other visual depictions of children or literature describing sexual contact with children. The overriding motivation for the collection of child pornography and erotica is to define, fuel, and validate the collector's most cherished sexual fantasies involving children. Visual depictions may range from fully clothed children engaged in non-sexual activity to nude children engaged in explicit sexual activity.

9. Individuals who collect child pornography tend to treat their material as prized possessions and are especially unlikely to part with them. Even if the collector feels threatened by exposure to law enforcement, he will usually seek to preserve his collection by hiding it better, rather than by destroying it. The collection may be culled and refined, but the size of the collection tends to increase over time. This is particularly true since digital storage media have increased in storage capacity as they have decreased in cost.

10. In fact, many collectors protect their collections by creating back-ups, sometimes multiple back-ups, of some or all of the collection. Child pornography, unlike some other kinds of contraband (e.g. drugs), is not "consumed" by the user. The "consumption" of this product results in its proliferation, more copies are generated. The very nature of computers as a means of collection, transmission, and/or storage lends itself to permanent preservation of the item. If the collector relocates, his collection almost always moves with him.

11. Individuals who collect child pornography tend maintain and possess their material in the privacy and security of their homes or some other secure location where it is readily available. The collection may include sexually explicit or suggestive materials involving

children, such as photographs, digital images, magazines, narratives, motion pictures, DVDs, CD ROMs, video tapes, books, slides, drawings, computer images or other visual media.

12. Based on my training and experience, I know that collectors of child pornography may also store their child pornography on digital cameras. Some child pornographers also produce child pornography using digital cameras.

INVESTIGATION OF NEIL MORGAN

13. The following outlines the investigation of Neil Morgan and his alleged use of the Internet a and computers to receive and store child pornography.

A. On July 17, 2007, a federal search warrant for the MORGAN residence:1601 Drew Rd, El Centro, CA (refer to U.S. Magistrate case number 07MJ8622) was executed. The search was for child pornography and was based on probable cause received from Internet searches previously performed by ASAC/CA as part of Operation Peer Precision. It had been determined that there was probable cause to believe that child pornography videos were being stored and distributed from computers in the residence.

B. One of the laptop computers, a Fujitsu Notebook, seized from the residence belonged to Neil MORGAN. Neil MORGAN's ownership of the computer was confirmed by witnesses in the house during the warrant, to include Neil MORGAN's father and brother. During a subsequent interview, Neil MORGAN also confirmed that the computer belonged to him.

C. During a subsequent forensic analysis of the Fujitsu laptop, ICE Digital Forensic Agent Rick Steele discovered over one thousand alleged images and videos of child pornography. These images and videos have been viewed by your Affiant. These images include depictions of prepubescent children as young as 6-7 years of age. The children are photographed in sexual poses and are receiving and giving vaginal, anal and oral sex to adult males.

D. Your Affiant has interviewed at least three witnesses who have seen Neil MORGAN's collection of child pornography. One of these witnesses further claims that her 10 year-old daughter was sexually molested by Neil MORGAN. The alleged child victim also reported the molest to law enforcement. One witness also reported to law enforcement that Neil MORGAN had confessed to her that he had molested the child. Charges for the child molest were filed in the State of Oregon.

E. Moreover, investigation revealed that Neil Morgan possessed another laptop computer other than the one found during the initial search warrant on July 17, 2007. During the initial search warrant executed on July 17, 2007 only one laptop belonging to Neil was found at the premises. The laptop that was found on July 17, 2007 was purchased after witnesses observed NEIL MORGAN with the other laptop.

F. Your Affiant interviewed Neil MORGAN on December 5, 2007, and learned that Neil MORGAN was aware that child pornography was on his computer. He stated that he viewed it out of curiosity and out of a desire to become a law enforcement investigator that goes after the people who make the illicit material. Neil MORGAN further stated that since his Fujitsu laptop was seized that he has not acquired another computer and that he does not even use computers any more. He said that his girlfriend checks his email for him.

G. On December 5, 2007, at approximately 1430 hours, ASAC/CA agents executed an arrest warrant at the MORGAN residence in order to arrest Neil MORGAN's brother, Nathan MORGAN, who was also allegedly in possession of child pornography. During the execution of the warrant a security sweep of the house was conducted. ASAC/CA Special Agents Mathew Kelley and Nicole Yammine entered Neil MORGAN's bedroom and immediately noticed in plain view, a laptop computer sitting on the bad. The laptop had power running to it and was opened. It was dark in color. Agents also identified a digital camera in close proximity of the laptop.

H. Also during the execution of the arrest warrant, Nathan MORGAN signed a Consent to Search form. ASAC/CA then identified a computer in Nathan MORGAN's bedroom. The computer was turned on and the screen displayed an Internet-based chat room or instant messaging program, indicating that the Internet was still active at the MORGAN residence.

I. Earlier on that day, December 5, 2007, at approximately 1130 hours, Your Affiant telephoned the MORGAN residence looking for Neil MORGAN in order to confirm the time of scheduled interview that afternoon at the ASAC/CA office. Nathan MORGAN answered the phone and went to find Neil MORGAN. Your Affiant heard Nathan MORGAN knocking on what appeared to be a door and calling for Neil. Nathan MORGAN returned to the phone and told Your Affiant that Neil was not answering the bedroom door. Approximately two and a half hours later, ASAC/CA agents, who had been conducting surveillance on the MORGAN residence since 0800 hours that morning, saw Neil MORGAN leave the residence and drive his car away.

Background on Computers

14. The term "computer" as used here is defined as 18 U.S.C. § 1030(e)(1), and includes electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such a device. As an ICE agent assigned to the Cybercrimes Division, I have had training in the investigation of computer-related crimes. Based upon my experience and knowledge, I know there are several reasons why a complete search and seizure of information from computers often requires seizure of all electronic storage devices, as well as all related peripherals, to permit a thorough search later by qualified computer forensic agents or experts in a laboratory or other controlled environment:

A. Computer storage devices, such as hard disks, diskettes, tapes, laser disks, compact discs, and DVDs, can store the equivalent of hundreds of thousands of pages of information. Additionally, when an individual seeks to conceal information that may constitute criminal evidence, that individual may store the information in random order with deceptive file names. As a result, it may be necessary for law enforcement authorities performing a search to examine all the stored data to determine which particular files are evidence or instrumentalities of criminal activity. This review and sorting process can take weeks or months, depending on the volume of data stored, and would be impossible to attempt during a search on site; and

B. Searching computer systems for criminal evidence is a highly technical process, requiring specialized skill and a properly controlled environment. The vast array of computer hardware and software available requires even those who are computer experts to specialize in some systems and applications. It is difficult to know before a search what type of hardware and software are present and therefore which experts will be required to analyze the subject system and its data. In any event, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to inadvertent or intentional modification or destruction (both from external sources or from destructive code imbedded in the system as a booby trap), a controlled environment is essential to its complete and accurate analysis.

15. Based on my own experience and my consultation with other agents who have been involved in computer searches, searching computerized information for evidence or instrumentalities of a crime often requires the seizure of all of a computer system's input and output peripheral devices, related software, documentation, and data security devices (including passwords) so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. There are several reasons that compel this conclusion:

A. The peripheral devices that allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output devices in order to read the data on the system. It is important that the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence listed above. In addition, the analyst needs the relevant system software (operating systems, interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices; and

B. In order to fully retrieve data from a computer system, the analyst also needs all magnetic storage devices, as well as the central processing unit (CPU). In cases like the instant one where the evidence consists partly of image files, the monitor and printer are also essential to show the nature and quality of the graphic images which the system could produce. Further, the analyst again needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media) for proper data retrieval.

C. I am familiar with and understand the implications of the Privacy Protection Act ("PPA"), 42 U.S.C. § 2000aa, and the role of this statute in protecting First Amendment activities. I am not aware that any of the materials to be searched and seized from the SUBJECT PREMISES are protected materials pursuant to the PPA. If any such protected materials are inadvertently seized, all efforts will be made to return these materials to their authors as quickly as possible.

Computer Search Protocol

16. With the approval of the court in signing this warrant, agents executing this search

warrant will employ the following procedures regarding computers that may be found at the premises which many contain information subject to seizure pursuant to this warrant:

A. There is probable cause to believe that the computer used to receive and send child pornography and sexually explicit images involving minors described herein constitute "property used in committing a crime" with the meaning of Rule 41(c)(3), Federal Rules of Criminal Procedure. Consequently, such computer(s) are subject to seizure. In addition, images of children engaged in sexually explicit conduct stored on the subject computer(s) are illegally possessed. The computer equipment, digital storage media, modems, keyboards, monitors and any peripherals discovered during the search will be seized and transported offsite for imaging and if such equipment contains images of children engaged in sexually explicit conduct will be retained as instrumentalities and as illegally possessed data. The digital media will be imaged for analysis, but the computer equipment will not be returned. Should the owner of the computer seek the return of any legal computer files or documents, the owner shall make such a request in writing to the U.S. Attorney's Office and shall include the names of specific file and/or documents sought. The U.S. Attorney's Office shall forward such written request to ICE and every attempt will be made to capture and return only the files and/or documents requested within 60 days of the written request.

B. A forensic image is an exact physical copy of the hard drive or other media. It is essential that a forensic image be obtained prior to conducting any search of the data for information subject to seizure pursuant to this warrant. A forensic image captures all of the data on the hard drive or other media without the data being viewed and without changing the data in anyway. This is in sharp contrast to what transpires when a computer running the common Windows operating system is started, if only to peruse and copy data - data is irretrievably changed and lost. Here is why: When a Windows computer is started, the operating system proceeds to write hundreds of new files about its status and operating environment. These new files may be written to places on the hard drive that may contain deleted or other remnant data. That data, if overwritten, is lost permanently. In addition, every time a file is accesses, unless the access is done by trained professionals using special equipment, methods and software, the operating system will re-write the metadata for that file. Metadata is information about a file that the computer uses to manage information. If an agent merely opens a file to look at it, Windows will overwrite the metadata which previously reflected the last time the file was accessed. The lost information may be critical.

C. Special software, methodology and equipment is used to obtained forensic images. Among other things, forensic images normally are "hashed", that is, subjected to a mathematical algorithm to the granularity of 10^{38} power, an incredibly large number much more accurate than the best DNA testing available today. The resulting number, known as a "hash value" confirms that the forensic image is an exact copy of the original and also serves to protect the integrity of the image in perpetuity. Any change, no matter how small, to the forensic image will affect the has value so that the image can no longer be verified as a true copy.

D. Forensic Analysis: After obtaining a forensic image, the data will be analyzed. Analysis of the data following the creation of the forensic image is a highly technical process that requires thousands of different hardware items and software programs that can be commercially purchased, installed and custom-configured on a user's computer system. Computers are usually customized by their users. Even apparently identical computers in an office environment can be significantly different with respect to configuration, including permissions and access rights, passwords, data storage and security. It is not unusual for a computer forensic examiner to have to obtain specialized hardware or software, and train with it, in order to view and analyze imaged data.

E. Analyzing the contents of a computer, in addition to requiring special technical skills, equipment and software also can be very tedious. It can take days to properly search a single hard drive for specific data. Searching by keywords, for example, often yields many thousands of "hits," each of which must be reviewed in its context by the examiner to determine whether the data is within the scope of the warrant. Merely finding a relevant "hit" does not end the review process. As mentioned above, the computer may have stored information about the data at issue: who created it, when it was created, when was it last accessed, when was it last modified, when was it last printed and when it was deleted. Sometimes it is possible to recover an entire document that was never saved to the hard drive if the document was printed. Operation of the computer by non-forensic technicians effectively destroys this and other trace evidence. Moreover, certain file formats do not lend themselves to keyword searches. Keywords search text. Many common electronic mail, database and spreadsheet applications do not store data as searchable text. The data is saved in a proprietary non-text format. Microsoft Outlook data is an example of a commonly used program which stores data in non-textual, proprietary manner-ordinary keyword searches will not reach this data. Documents printed by the computer even if the document was never saved to the hard drive, are recoverable by forensic examiners but not discoverable by keyword searches because the printed document is stored by the computer as a graphic image and not as text. Similarly, faxes sent to the computer are stored as graphic images and not as text.

F. Analyzing data on-site has become increasingly impossible as the volume of data stored on a typical computer system has become mind-boggling.

For example, a single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double spaced pages of text. Computer hard drives are now capable of storing more than 100 gigabytes of data and are commonplace in new desktop computers. And, this data may be stored in a variety of formats or encrypted. The sheer volume of data also has extended the time that it takes to analyze data in a laboratory. Running keyword searches takes longer and results in more hits that must be individually examined for relevance. Even pursuing only a directory listing of a home computer can result in thousands of pages of printed material most of which likely will be limited probative value.

G. Based on the foregoing, searching any computer or forensic image for the information subject to seizure pursuant to this warrant may require a range of data analysis techniques and may take weeks or even months. Keywords need to be modified continuously based upon the results obtained; criminals can mislabel and hide files and directories, use codes to avoid using keywords, encrypt files, deliberately misspell certain words, delete files and take other steps to defeat law enforcement. In light of these difficulties, I request permission to use whatever data analysis techniques reasonably appear necessary to locate and retrieve digital evidence within the scope of this warrant.

H. All forensic analysis of the imaged data will be directed exclusively to the identification and seizure of information with the scope of this warrant. In the course of proper examination, the forensic examiner may view information not within the scope of the warrant. Such information will not be made available to the investigating agents unless it appears to the examiner that the information relates to the commission of offenses not covered by this warrant. In that event, the examiner will confer wit the investigator so that the investigator can determine whether to seek a further search warrant for newly uncovered data.

17. In conclusion, based upon the information contained in this affidavit, your Affiant has reason to believe that images, records, evidence, fruits and instrumentalities relating to violations of Title 18, United States Code, §2252 et seq exists. Your Affiant further believes that images, records, evidence, fruits and instrumentalities are located on a laptop computer and a digital camera within the bedroom of Neil MORGAN at the residence located at 1601 Drew Rd, Lot 39, El Centro, CA, more particularly described in Attachment "A".

Senior Special Agent Timothy Ballard

Subscribed to and sworn before me this 6th day of December, 2007

The Honorable Peter C. Lewis
UNITED STATES MAGISTRATE JUDGE